

**REMARKS**

Applicants thank the Examiner for participating in an interview with Applicants' representative on March 31, 2004. During the interview, the claims were discussed and Applicant advanced several arguments over the cited references. As the Examiner requested, Applicants submit this Reply to Office Action to formally set forth those arguments.

As a preliminary matter, Applicants affirm the oral election made on January 8, 2004, electing to prosecute claims 1-4 and 7-14, characterized by the Examiner as drawn to network security. By this Amendment, Applicants withdraw claims 5 and 6 from consideration at this time.

*Information Disclosure Statements*

In the Office Action, the Examiner stated that many of the references cited by Applicants in Information Disclosure Statements are missing from the file at the Patent Office. However, during the interview on March 31, 2004, the Examiner stated that the missing references had been located at the Patent Office and that he would consider them and return the completed 1449 forms to indicate that he has done so.

*Section 102 Rejections*

In the Office Action, the Examiner rejected claims 1, 2, 12, and 13 under 35 U.S.C. § 102(e) as anticipated by Touboul, U.S. Patent No. 6,092,194 ("Touboul '194"). The Examiner also rejected claims 3, 4, 7-11, and 14 under 35 U.S.C. § 102(e) as anticipated by Touboul, U.S. Patent No. 6,154,844 ("Touboul '844").

To anticipate a claim under 35 U.S.C. § 102, the reference must teach every element of the claim. M.P.E.P. § 2131.01 (8<sup>th</sup> ed. 2001, revised February 2003). the Examiner failed to show that Touboul '194 teaches several elements of claims 1, 2, 12, and 13. Therefore, Applicants request the reconsideration and withdrawal of the section 102 rejections of these claims.

Touboul '194 discloses a “system for protecting a network from suspicious Downloadables” by applying a security policy to a Downloadable to determine whether the security policy has been violated. (Touboul '194, col. 1, ll. 60-65.) To apply the security policy to the Downloadable, the system of Touboul '194 compares data about the Downloadable to a list of known hostile Downloadables, access control lists, trusted certificates, or trusted URLs. (Id., col. 2, ll. 11-20.) If the Downloadable passes these tests, it is sent to its intended recipient. (Id., col. 6, ll. 62-65.)

Claim 1 recites, among other things, downloading code from a server and determining a set of constraints to implement secure communication with the server. The Examiner failed to show that Touboul '194 discloses this combination of steps. Instead, the security policies disclosed in the reference are “policies for determining whether to allow or block an incoming Downloadable.” (Touboul '194, col. 4, ll. 18-21.) As described above, the security policies of the reference merely compare data about the Downloadable to lists of known hostile programs, trusted certificates, trusted URLs, etc. They have nothing to do with determining constraints to implement secure communication with the server from which code was downloaded.

The Examiner also failed to show that Touboul '194 teaches using secure code to verify that downloaded code will enforce the set of constraints when the downloaded code is used to communicate with the server. Instead, the security system of the reference compares a Downloadable ID to a security policy to determine whether to send the Downloadable to its intended recipient. Comparing an identifier of the Downloadable to a security policy to determine whether to send the Downloadable to its intended recipient is unrelated to using secure code to verify that downloaded code will enforce the set of constraints when the downloaded code is used to communicate with the server. Furthermore, even if the security policy of the reference can be interpreted as the claimed set of constraints, the security policy is enforced by the security system of the reference, not by downloaded code. (Touboul '194, col. 4, ll. 45-47.)

Because the Examiner has not shown that Touboul '194 teaches every element of claim 1, the section 102 rejections of claim 1 and its dependent claim 2 should be withdrawn.

Claim 12 recites a computer-readable medium containing instructions for controlling a data processing system to perform the method described in claim 1. Therefore, for at least the reasons given above with respect to claim 1, the Examiner has not shown that Touboul '194 teaches every element of claim 12, and Applicants request the reconsideration and withdrawal of the section 102 rejections of claim 12 and its dependent claim 13.

Claim 2 further recites using downloaded code to invoke a method on the server, wherein the downloaded code enforces the set of constraints on the server. The

Examiner failed to show that Touboul '194 teaches this step. Instead, the reference teaches security policies used to determine whether to allow or block incoming Downloadables. (Touboul '194, col. 4, ll. 18-21.) Even if the security policies of the reference can be construed as the claimed set of constraints, the security policies of Touboul '194 are used to determine whether to block the Downloadable. (Id.) They are not enforced by the downloaded code. Because the Examiner did not show that Touboul '194 teaches this additional element of claim 2, the section 102 rejection of claim 2 should be withdrawn.

Claim 13 recites a computer-readable medium containing instructions for controlling a data processing system to perform a method including the step recited in claim 2. Therefore, the Examiner has not shown that Touboul '194 teaches this additional element of claim 13, and the section 102 rejection of claim 13 should be withdrawn.

The Examiner relied on Touboul '844 to reject claims 3, 4, 7-11, and 14 under 35 U.S.C. § 102(3). However, the Examiner failed to show that the reference teaches several elements of these claims, and Applicants request the reconsideration and withdrawal of the section 102 rejections of claims 3, 4, 7-11, and 14.

Touboul '844 discloses a system for attaching a security profile to a Downloadable to protect computers from hostile Downloadables. (Touboul '844, co. 1, ll. 23-27.) In particular, the reference discloses a content inspection engine that generates a Downloadable security profile and links it to the corresponding Downloadable. (Id., col. 2, ll. 3-9.) A protection engine examines the Downloadable

security profile to determine whether to trust the profile and compares the security profile to a security policy. (Id., col. 2, ll. 20-29.) In one embodiment, multiple inspection engines may generate multiple security profiles for a Downloadable. (Id., col. 12-14; col. 12, ll. 15-22.)

Claim 3 recites a method including the steps of downloading a first proxy containing code for communication purposes and using the first proxy to obtain a second proxy containing code for communication purposes. In the Office Action, the Examiner stated that the security profiles of the reference taught the first proxy and the second proxy of claim 3. (1/14/04 Office Action, p. 5.) However, this interpretation contradicts the express teachings of the reference. First, the security profiles of the reference do not contain code for communication purposes. Instead, the security profiles include "a list of all potentially hostile or suspicious computer operations that may be attempted by the Downloadable, and may also include the respective arguments of those operations." (Touboul '844, col. 4, ll. 4-7.) Second, the security profiles of Touboul '844 are not downloaded, they are generated by a content inspection engine. (Touboul '844, col. 2, ll. 3-5.)

Even if the security profiles of the reference could be interpreted as the first proxy and second proxy of claim 3, there is no teaching in the reference that one security profile is used to obtain a second security profile. Instead, the reference teaches that additional content inspection engines may be included for generating additional security profiles for a Downloadable. (Touboul '844, col. 2, ll. 12-15.) Therefore, the Examiner has not shown that Touboul '844 teaches a method including the steps of downloading

a first proxy containing code for communication purposes and using the first proxy to obtain a second proxy containing code for communication purposes.

Claim 3 further recites the step of determining whether a server is trustworthy by using the second proxy. The Examiner has also failed to show that Touboul '844 teaches this step. As discussed above, the reference teaches only using a security profile to determine whether to trust a Downloadable. There is simply no teaching of determining whether a server is trustworthy in the reference. Furthermore, under the Examiner's interpretation of the reference, the second proxy is a security profile linked to a Downloadable and used to determine whether the Downloadable may be trusted. The security profile is not used to determine whether a server is trustworthy.

Claim 3 also recites the step of requesting the server to determine whether the first proxy is trustworthy by using the second proxy. The Examiner did not mention this step in the Office Action or allege any teaching of it in Touboul '844. Furthermore, the second proxy cannot be interpreted as the security policy of the reference because the security policy is used to determine whether a Downloadable can be trusted, not whether a server is trustworthy. The second proxy also cannot be interpreted as the Downloadable of the reference because the Downloadable is not used to determine whether a server is trustworthy.

Because the Examiner has failed to show that Touboul '844 discloses each and every element recited in claim 3, Applicants request the reconsideration and withdrawal of the section 102 rejections of claim 3 and its dependent claim 4.

Claim 14 recites a computer-readable medium containing instructions for controlling a data processing system to perform the method recited in claim 3.

Therefore, for at least the reasons given above with respect to claim 3, the Examiner has failed to show that Touboul '844 discloses several elements of claim 14, and Applicants request the reconsideration and withdrawal of the section 102 rejection of claim 14.

Finally, claim 7 recites a client computer comprising a memory with a proxy and a secure verifier that can be used to verify that the proxy will enforce security constraints when communicating with a service. The Examiner has not shown that Touboul '844 teaches such a structure. Instead, the reference teaches a client computer including a web client for communicating with a web server. (Touboul '844, Fig. 1, col. 5, ll. 5-13.) A computer protection engine examines a security profile of a Downloadable. (Id., col. 7, ll. 51-67.) However, as discussed above, the security profiles of the reference are “a list of all potentially hostile or suspicious computer operations that may be attempted by the Downloadable, and may also include the respective arguments of those operations.” (Touboul '844, col. 4, ll. 4-7.) Thus, examining a security profile is unrelated to verifying that a proxy will enforce security constraints when communicating with a service, as recited in claim 7. Because the Examiner has not shown that Touboul '844 teaches every element of claim 7, Applicants request the reconsideration and withdrawal of the section 102 rejections of claim 7 and its dependent claims 8-11.

In view of the foregoing amendments and remarks, Applicants respectfully request reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,  
GARRETT & DUNNER, L.L.P.

Dated: April 13, 2004

By: 

Jeffrey A. Berkowitz  
Reg. No. 36,743